Proposal Topic

BitCoin & Ethereum Network Analysis

Shiv Raj Pant, Xiaoqin Fu

School of Electrical Engineering and Computer Science

Washington State University

Pullman, WA

Email: {shiv.pant, xiaoqin.fu}@wsu.edu

I. Introduction

BitCoin was developed in 2008 and 2009 [1] using blockchain technology. Our research focuses on study data from a BITCOIN marketplace with interactions and ratings [2]. They are (directed) weighted signed network (WSN) in which edge corresponds to some weight, the rating from user u to user v [3]. They forms webs of trust between users allowing two unknown users to perform a transaction based on the aggregated trust [3].

Similar to Bitcoin, Ethereum is an open-source, public, decentralized platform to run smart contracts on a custom built blockchain. Its enables developers to store registries of promises or debts, move funds and create markets. The Ethereum project was bootstrapped in 2014 and is developed by the Ethereum Foundation, a Swiss non-profit [4]. ERC-20 is a technical standard developed in late 2015 on the Ethereum blockchain for smart contracts [5]. It defines rules for Ethereum tokens within the larger Ethereum network, including transfer methods for the tokens between addresses and transfer methods [5].

II. Methodology

Our paper is to study and analyze the two trust networks: Bitcoin OTC web of trust network and Bitcoin Alpha web of trust network. Moveover, we will analyze ethereum ERC-20 token transfer network. For the experiment, we will extract both topological and non-topological features from the networks [6] [7] [8].

III. DATA

We will use two data sets, soc-sign-bitcoin-otc and soc-sign-bitcoin-alpha, from [9]. OTC and Alpha are two Bitcoin exchanges, which are open market websites allowing users to buy and sell things [9]. The soc-sign-bitcoin-otc, Bitcoin OTC web of trust network, is a (directed) weighted signed network (WSN) with 5,881 nodes and 35,592 edges. On Bitcoin OTC, people can build up trust to exchange bitcoins with ratings from -10 (total distrust) to 10 (total trust) which are associated with how much a user trusts another user [3]. A high rating is mapping the high trust. The data set has the rating times recorded as seconds since Epoch [9].

And the soc-sign-bitcoin-alpha, Bitcoin Alpha web of trust network, is also a directed WSN with 3,783 nodes and 24,186 edges. It is similar in almost every way to the soc-sign-bitcoin-otc. It also has ratings from -10 to 10 and the rating times. While the OTC network is still active, the Alpha exchange is no longer active now [3].

We also downloaded ETC-R20 data set and define the token network, in which each node is an address and each edge represents the transfer of the amount of the respective token between two addresses [10]. The data set 190 nodes and 3000 edges, whose data are from 2019/01/01. We will download more ETC-R20 data sets with different time stamps.

IV. RELATED WORK

A. Blockchain

Blockchain is a distributed database to keep records. A block encrypts the data using cryptographic hash function, such as SHA-256, and keeps record of next available block for traversing the blocks. Records are stored in a tree structure where the leaves stores the transaction information and other intermediate nodes store the hash values. The root of this tree belongs in a block containing the hash value generated from child nodes. The timestamp in a block is used to synchronize the position of a block in blockchain. A block also contains NONCE value, which is random unique number for a specific block.

B. Blockchain network analysis

A blockchain can be separated to two layers from a graph-centric perspective: a network layer and an application layer. They can be represented by a communication graph and a content graph. For the analysis of content graphs, social network analysis techniques are commonly used. Many cryptocurrency-based

approaches analyze content graphs relying on assumptions and ways of social network analysis. A content graphs can be modelled on three networks: a transaction network, address network and user/entity network. In transaction networks, the nodes are transactions, and the edges represent the flow of transferred assets. In an address network, the nodes are addresses, and a edges is a transaction between two of addresses. In a user/entity network, the nodes are real-world users/entities while the edges show the value flows [10].

C. IOTA network

IOTA (the Internet of Things Applications) network is an alternate of Bitcoin and it used tangle technology as a distributed ledger instead of Blockchain. The network is a directed acyclic graph where each node indicates an entity that issue and validate transaction [11]. The edge indicates the relationship between a new transaction and the old transaction. The direction of an edge is from a new transaction to one of the recent transactions. In order to approve a new transaction, tangle verify most recent two transactions, hence, each node points to at most two previous nodes in terms of time.

V. TENTATIVE PLAN

- Bitcoin OTC web of trust network analysis
- Bitcoin Alpha web of trust network analysis
- ETC-R20 token network analysis

REFERENCES

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[2] E. H. Aw, R. Gera, K. Hicks, N. Koeppen, and C. Teska, "Analyzing preferential attachment in peer-to-peer bitcoin networks," in *2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*. IEEE, 2018, pp. 1242–1249.

[3] O. Moindrot, "Trust in bitcoin exchange networks," 2017.

[4] "ethereum," https://www.ethereum.org/.

[5] Wikipedia, "Erc-20," https://en.wikipedia.org/wiki/ERC-20#cite_note-:0-1, 2019.

[6] D. Liben-Nowell and J. Kleinberg, "The link-prediction problem for social networks," *Journal of the American society for information science and technology*, vol. 58, no. 7, pp. 1019–1031, 2007.

[7] M. Al Hasan, V. Chaoji, S. Salem, and M. Zaki, "Link prediction using supervised learning," in *SDM06: workshop on link analysis, counter-terrorism and security*, 2006.

[8] D. Davis, R. Lichtenwalter, and N. V. Chawla, "Multi-relational link prediction in heterogeneous information networks," in *2011 International Conference on Advances in Social Networks Analysis and Mining*. IEEE, 2011, pp. 281–288.

[9] J. Leskovec and A. Krevl, "SNAP Datasets: Stanford large network dataset collection," http://snap.stanford.edu/data, Jun. 2014.

[10] F. Victor and B. K. Lüders, "Measuring ethereum-based erc20 token networks."

[11] S. Popov, "The tangle," *cit. on*, p. 131, 2016.